

SET RECONSTRUCTION ON THE HYPERCUBE

LUKE PEBODY

ABSTRACT. Given an action of a group G on a set S , the k -deck of a subset T of S is the multiset of all subsets of T of size k , each given up to translation by G .

For a given subset T , the *reconstruction number* of T is the minimum k such that the k -deck uniquely identifies T up to translation by G , and the *reconstruction number* of the action $G : S$ is the maximum reconstruction number of any subset of S .

The concept of reconstruction number extends naturally to multisubsets T of S and in [2], the author calculated the multiset-reconstruction number of all finite abelian groups. In particular, it was shown that the multiset-reconstruction number of \mathbb{Z}_2^n was $n+1$. This provides an upper bound of $n+1$ to the reconstruction number of \mathbb{Z}_2^n . The author also showed a lower bound of $\lfloor \frac{n+1}{2} \rfloor$ in the same paper.

The purpose of this note is to close the gap. The reconstruction number of \mathbb{Z}_2^n is

$$\lfloor n+1 - \log_2(n+1 - \log_2(n)) \rfloor.$$

1. INTRODUCTION AND DEFINITIONS

Given a set S and non-negative integer k , denote by $S^{(k)}$ the set of subsets of S of size k . Given an action on a group G of a set S , the k -deck of a subset T is the multiset of all subsets of T of size k , each given up to translation by G :

$$\text{deck}_k(G) = \{\{gU : g \in G\} : U \in T^{(k)}\}.$$

Say that subsets T_1 and T_2 are k -indistinguishable if $\text{deck}_i(T_1) = \text{deck}_i(T_2)$ for all $i \leq k$ and k -distinguishable otherwise. In particular, for any subset T of G , any element g of G and any integer k , gT and T are k -indistinguishable and sets T_1 and T_2 are k -indistinguishable if and only for all $i \leq k$, there is a bijection $\phi_i : T_1^{(i)} \rightarrow T_2^{(i)}$ such that for all $U \in T_1^{(i)}$ there exists a g such that $\phi_i U = gU$.

For subsets T_1 and T_2 say that the *distinguishing number* of T_1 and T_2 , denoted by $d_{G:S}(T_1, T_2)$, is the smallest number k such that T_1 and T_2 are k -distinguishable. If there is no such k (and so T_1 and T_2 are translates), the distinguishing number is ∞ .

For a subset T of S , say that the *reconstruction number* $r_{G:S}(T)$ is the smallest number k such that for any subset U of S , if T and U are k -indistinguishable then U is a translate gT of T , and the *reconstruction number* $r(G : S)$ is the maximum value of $r_{G:S}(T)$ for any subset $T \subseteq S$.

One can extend the definition of reconstruction from sets to multisets. Let a *multiset* from S be a map $\phi : S \rightarrow \mathbb{N}$ from S to the non-negative integers \mathbb{N} , and then define the k -deck of ϕ to be the map $\text{deck}_k \phi : S^k \rightarrow \mathbb{N}$ defined by

$$\text{deck}_k(s_1, s_2, \dots, s_k) = \sum_{g \in G} \phi(gs_1) \phi(gs_2) \dots \phi(gs_k).$$

Given this definition of a k -deck, we can define k -distinguishable and k -indistinguishable as before, and for a multiset ϕ from G , say that the multiset reconstruction number $\text{rm}_{G:S}(\phi)$ is the smallest number k such that for any multiset ψ from G , if ϕ and ψ are k -indistinguishable, then ψ is a translate $g\phi$ (defined by $g\phi(s) = \phi(g^{-1}s)$) of ϕ . Finally, define the multiset reconstruction number $\text{rm}(G : S)$ to be the maximum value of $\text{rm}_{G:S}(\phi)$ for any multiset ϕ from G .

One of the first general results in this area was in [1], where the authors showed that the reconstruction number of a group action $r(G : S)$ was bounded above by $\log_2(|G|)$.

In this paper we will focus on the action of an abelian group acting on itself by multiplication. For the specific case of the cyclic group acting on itself by multiplication, it was proved in [3] that the reconstruction number of $r(\mathbb{Z}_n)$ was at most equal to 9 times the number of prime factors of n and was equal to 3 for prime n . This was improved upon in [2] where the multiset reconstruction number was calculated for every abelian group and, thereby, it was shown that $r(\mathbb{Z}_n) \leq 6$.

We will focus on the group \mathbb{Z}_2^n which we will identify both, where necessary, with the n -dimensional vector space over the field of 2 elements and with the power set of the n element set. In [2], it was shown that the multiset reconstruction number of \mathbb{Z}_2^n is $n + 1$, from which it follows that $r(\mathbb{Z}_2^n) \leq n + 1$. In the same paper, a lower bound was provided of $\frac{n+1}{2}$. In this paper we will show that the reconstruction number is equal to $\lfloor n + 1 - \log_2(n + 1 - \log_2(n)) \rfloor$. This expression may seem a tad unwieldy, but comes from the following fact.

Theorem 1. *For positive integers n and k , the statements*

$$k \leq \lfloor n + 1 - \log_2(n + 1 - \log_2(n)) \rfloor$$

and

$$2^{n+1-k} \geq k$$

are equivalent.

Proof. Let us suppose that t is the unique non-negative integer that $2^t + t \leq n < 2^{t+1} + t + 1$. Then if we set $k = n - t$, we see that $2^{n+1-k} = 2^{t+1} \geq n - t = k$, but if we set $k = n + 1 - t$, we see that $2^{n+1-k} = 2^t < n + 1 - t = k + 1$. Since 2^{n+1-k} is decreasing in k , it follows that $2^{n+1-k} \geq k$ if and only if $k \leq n - t$.

Further, if $2^t + t \leq n < 2^{t+1}$, then $\log_2(n)$ is between t and $t + 1$, so $n + 1 - \log_2(n)$ is between 2^t and 2^{t+1} . Similarly, if $2^{t+1} \leq n < 2^{t+1} + t + 1$, then $\log_2(n)$ is between $t + 1$ and $t + 2$, so $n + 1 - \log_2(n)$ is between 2^t and 2^{t+1} .

It follows that $\lfloor n + 1 - \log_2(n + 1 - \log_2(n)) \rfloor = n - t$. \square

In Section 2, we will show that if $2^{n+1-k} \geq k$ then the reconstruction number of \mathbb{Z}_2^n is at least k , and in Sections 3 and 4, we will show the converse.

2. LOWER BOUND

To prove our lower bound, we provide a method for creating sets which are not easily distinguishable.

Theorem 2. *Suppose that G contains a subgroup H , and that set A is the union of sets A_1, \dots, A_k such that for each i , A_i is contained in a distinct coset $g_i H$ of H .*

Suppose likewise that set B is the union of sets B_1, \dots, B_k such that for each i , B_i is contained in a distinct coset $g'_i H$ of H .

Suppose finally that for each $1 \leq i \leq k$, $A \setminus A_i$ and $B \setminus B_i$ are translates. Then A and B are not $k - 1$ -distinguishable.

Proof. Let g_1, g_2, \dots, g_i (with $i < k$) be elements of G , and for set $S \subseteq G$ denote by $f(S)$ the number of elements g of G for which $gg_1, gg_2, \dots, gg_i \in S$.

Let t be the number of distinct cosets of H in which g_1, g_2, \dots, g_i lie. Note that $t \leq i < k$. Then for any g , gg_1, gg_2, \dots, gg_i lie in t cosets of H . Therefore each version gg_1, gg_2, \dots, gg_i contained in A is contained in exactly $k - t$ of the sets $A \setminus A_j$.

Thus $(k - t)f(A) = \sum_i f(A \setminus A_i) = \sum_i f(B \setminus B_i) = (k - t)f(B)$ and hence $f(A) = f(B)$.

Since this is true for all g_1, g_2, \dots, g_i with $i \leq k$, it follows that A and B are not $(k - 1)$ -distinguishable. \square

Now we show how to find sets satisfying the properties of Theorem 2

Corollary 3. *For positive integer $k \geq 3$, suppose that abelian group G contains a subgroup H of index at least k . Suppose also that subgroup H has k cosets of subgroups $h_i H_i$ such that the intersection of the cosets is empty:*

$$\bigcap_i h_i H_i = \emptyset,$$

and all of the smaller intersections are not empty:

$$\forall j \bigcap_{i \neq j} h_i H_i \neq \emptyset.$$

Then the reconstruction number of G is at least k .

Proof. Since $\bigcap_i h_i H_i$ is different from $\bigcap_{i \neq j} h_i H_i$ for all j , it follows that the cosets $h_i H_i$ are distinct. Further, since for all pairs i, j , $h_i H_i \cap h_j H_j \neq \emptyset$, it follows that the subgroups H_i and H_j are distinct.

Choose k distinct cosets $g_1 H, g_2 H, \dots, g_k H$ of H in G , and then for $1 \leq i \leq k$, let $A_i = g_i H_i$ and let $B_i = g_i h_i H_i$. Finally let A be the disjoint union of the A_i and B be the disjoint union of the B_i .

Choose $1 \leq i \leq k$, and let x be any element of $\bigcap_{j \neq i} h_j H_j$. Then for all $j \neq i$, $x A_j = x g_j H_j = g_j x H_j = g_j h_j H_j = B_j$, and so $x(A \setminus A_i) = \bigcup_{j \neq i} x A_j = \bigcup_{j \neq i} B_j = B \setminus B_i$.

Thus the sets A_i and B_i satisfy the condition of Theorem 2, and hence A and B are not $k - 1$ -distinguishable. Further, we will show that A and B are not translates.

Suppose otherwise, then there exists $g \in G$ such that $gA = B$. Since cosets of H are preserved by the map $x \rightarrow gx$, it follows that this map must map each A_i to some B_j . However, if $i \neq j$ then A_i and B_j are cosets of different subgroups H_i and H_j which means one cannot be mapped to the other.

Thus for each i , it follows that $gg_i H_i = g_i h_i H_i$, from which it follows (since G is abelian) that $g \in h_i H_i$ for all i . This is a contradiction, as

$$\bigcap_i h_i H_i = \emptyset.$$

It follows that A and B are not $k - 1$ -distinguishable, and are not translates, so G must have reconstruction number of at least k . \square

To conclude we will show the existence of cosets with this intersection property.

Lemma 4. *The hypercube \mathbb{Z}_2^{k-1} contains k cosets of subgroups with empty intersection, such that the intersection of any $k - 1$ of them is not empty.*

Proof. Representing the elements of \mathbb{Z}_2^{k-1} as sequences $(x_1, x_2, \dots, x_{k-1})$ of elements of \mathbb{Z}_2 , we can take our k cosets $x_1 = 0$, $x_1 = x_2$, $x_2 = x_3$, \dots , $x_{k-2} = x_{k-1}$ and $x_{k-1} = 1$.

Clearly no vector satisfies all of these conditions, but if you remove any one condition, they can be satisfied. \square

This concludes the work for the lower bound.

Corollary 5. *If positive integers n, k have $2^{n+1-k} \geq k$ then the reconstruction number of \mathbb{Z}_2^n is at least k .*

Proof. For $k \geq 3$, this follows directly from Corollary 3 and Lemma 4. \mathbb{Z}_2^{k-1} is a subset of \mathbb{Z}_2^n of index 2^{n+1-k} , so if this is at least k , the conditions of Lemma 4 apply.

For $k = 1$ and $k = 2$, the conditions are that $2^{n-1} \geq 1$ and $2^{n-2} \geq 2$, which are both equivalent to $n \geq 2$.

For $n \geq 2$ and for any two non-zero elements a, b of \mathbb{Z}_n^2 the sets $\{0, a\}$ and $\{0, b\}$ are non-translates that are not 1-distinguishable so \mathbb{Z}_n^2 has reconstruction number at least 2. \square

3. THE FOURIER TRANSFORM

Given elements $x = (x_1, x_2, \dots, x_n)$ and $y = (y_1, y_2, \dots, y_n)$ of \mathbb{Z}_2^n , define $\langle x, y \rangle = (-1)^{x_1 y_1 + x_2 y_2 + \dots + x_n y_n}$. Then, given a mapping $f : \mathbb{Z}_2^n \rightarrow \mathbb{Z}$ the Fourier transform $\hat{f} : \mathbb{Z}_2^n \rightarrow \mathbb{Z}$ is defined by $\hat{f}(x) = \sum_{y \in \mathbb{Z}_2^n} f(y) \langle x, y \rangle$.

It is a well-known property of the Fourier Transform (which we will use in the proof of Theorem 10) that applying the Fourier Transform twice just multiplies the original map by the size of the group: $\hat{\hat{f}}(x) = 2^n f(x)$.

Given a multiset f from \mathbb{Z}_2^n and a linear map $\theta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^k$, denote by θf the multiset from \mathbb{Z}_2^k defined by

$$\theta f(x) = \sum_{z: \theta z = x} f(z).$$

For every linear map $\theta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^k$, there is a dual map $\theta^* : \mathbb{Z}_2^k \rightarrow \mathbb{Z}_2^n$ with the property that for every $x \in \mathbb{Z}_2^n$ and $y \in \mathbb{Z}_2^k$, $\langle \theta x, y \rangle = \langle x, \theta^* y \rangle$. The dual map gives a clean description of the Fourier transform of linear images of multisets.

Lemma 6. *Given a multiset f from \mathbb{Z}_2^n and a linear map $\theta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^k$ with dual θ^* , the Fourier transform of the image θf is given by*

$$\widehat{\theta f}(x) = \hat{f} \theta^* x.$$

Proof.

$$\begin{aligned} \widehat{\theta f}(x) &= \sum_{y \in \mathbb{Z}_2^k} \theta f(y) \langle x, y \rangle \\ &= \sum_{y \in \mathbb{Z}_2^k} \sum_{z: \theta z = y} f(z) \langle x, y \rangle \\ &= \sum_{z \in \mathbb{Z}_2^n} f(z) \langle x, \theta z \rangle \\ &= \sum_{z \in \mathbb{Z}_2^n} f(z) \langle \theta^* x, z \rangle \\ &= \hat{f} \theta^* x. \end{aligned}$$

\square

There is a similar easy to describe effect of translation on the Fourier Transform.

Lemma 7. *Given a multiset f from \mathbb{Z}_2^n and an element $z \in \mathbb{Z}_2^n$, the Fourier transform of the translate $z + f$ is given by*

$$(z + \hat{f})x = \hat{f}x \langle x, z \rangle.$$

Proof.

$$\begin{aligned}
(z \hat{+} f)x &= \sum_{y \in \mathbb{Z}_2^n} (z + f)(y) \langle x, y \rangle \\
&= \sum_{y \in \mathbb{Z}_2^n} f(z + y) \langle x, y \rangle \\
&= \sum_{y' \in \mathbb{Z}_2^n} f(y') \langle x, z + y' \rangle \\
&= \sum_{y' \in \mathbb{Z}_2^n} f(y') \langle x, z \rangle \langle x, y' \rangle \\
&= \langle x, z \rangle \sum_{y' \in \mathbb{Z}_2^n} f(y') \langle x, y' \rangle \\
&= \langle x, z \rangle \hat{f}x.
\end{aligned}$$

□

It is proved in [2] that the reconstruction number of a given multiset can be described in terms of the Fourier transform.

Theorem 8. *The k -deck of f gives exactly the same information as knowing all values $\prod_{i=1}^k \hat{f}(x_i)$ for all sequences (x_1, x_2, \dots, x_k) with $x_1 + x_2 + \dots + x_k = 0$.*

We can use this to show the effect of linear maps on distinguishability.

Theorem 9. *For any multisets f, g on \mathbb{Z}_2^n and integer $k \geq 2$:*

- (1) *If f and g are k -indistinguishable then for any linear map θ from \mathbb{Z}_2^n to any target space, θf and θg are k -indistinguishable.*
- (2) *If f and g are k -distinguishable, then there exists a linear map $\theta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{k-1}$ such that θf and θg are k -distinguishable.*

Proof. By Theorem 8, f and g being k -indistinguishable is equivalent to

$$\hat{f}(x_1) \dots \hat{f}(x_i) = \hat{g}(x_1) \dots \hat{g}(x_i)$$

for all sequences x_1, \dots, x_i with $i \leq k$ and $x_1 + \dots + x_i = 0$.

Suppose f and g are k -indistinguishable, and let $\theta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^p$ be any linear map. Then by Lemma 6, for any sequence $x_1, \dots, x_i \in \mathbb{Z}_2^n$ with $i \leq k$ and $x_1 + \dots + x_i = 0$,

$$\begin{aligned}
\hat{\theta f}(x_1) \dots \hat{\theta f}(x_i) &= \hat{f}(\theta^* x_1) \dots \hat{f}(\theta^* x_i) \\
&= \hat{g}(\theta^* x_1) \dots \hat{g}(\theta^* x_i) \\
&= \hat{\theta g}(x_1) \dots \hat{\theta g}(x_i),
\end{aligned}$$

so θf and θg are k -indistinguishable.

Similarly, for k -distinguishable f and g , there exists a sequence x_1, \dots, x_i with $i \leq k$, $x_1 + \dots + x_i = 0$ and

$$\hat{f}(x_1) \dots \hat{f}(x_i) \neq \hat{g}(x_1) \dots \hat{g}(x_i).$$

Then define map $\theta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{k-1}$ in terms of its dual by $\theta^* e_j = x_j$ for $j < i$ and $\theta^* e_j = 0$ for $j \geq i$. Note that $\theta^*(e_1 + \dots + e_{i-1}) = x_i$.

Thus if we let $y_j = e_j$ for $j < i$ and $y_i = e_1 + \dots + e_{i-1}$, then y_1, \dots, y_i are a sequence with $i \leq k$, $y_1 + \dots + y_i = 0$ and

$$\hat{\theta} f(y_1) \dots \hat{\theta} f(y_i) \neq \hat{\theta} g(y_1) \dots \hat{\theta} g(y_i),$$

so θf and θg are k -distinguishable. \square

4. STRUCTURE OF MAXIMALLY INDISTINGUISHABLE MULTISSETS ON \mathbb{Z}_2^{k-1}

For this section, we will investigate the nature of multisets from \mathbb{Z}_2^{k-1} which have distinguishing number k . We will give concrete examples of such multisets now.

For distinct non-negative integers a, b and positive integers a_1, \dots, a_{k-1} , denote by $f_{(a,b),(a_1,\dots,a_{k-1})}$ the multiset defined by

$$f((x_1, x_2, \dots, x_{k-1})) = \begin{cases} a + \sum a_i x_i & \text{if } \sum x_i \text{ is even} \\ b + \sum a_i x_i & \text{if } \sum x_i \text{ is odd} \end{cases}$$

We note that the Fourier Transform of $f_{(a,b),(a_1,\dots,a_{k-1})}$ takes a particularly simple form. Since the all-ones vector $e_1 + e_2 + \dots + e_{k-1}$ will come up quite a lot this section, denote it by h .

Theorem 10. *The Fourier Transform of $f_{(a,b),(a_1,\dots,a_{k-1})}$ is given by*

$$\hat{f}_{(a,b),(a_1,\dots,a_{k-1})}(x) = \begin{cases} 2^{k-2}(a + b + \sum a_i) & \text{if } x = 0 \\ 2^{k-2}a_i & \text{if } x = e_i \\ 2^{k-2}(a - b) & \text{if } x = h \\ 0 & \text{otherwise} \end{cases}$$

Proof. Let $g : \mathbb{Z}_2^{k-1} \rightarrow \mathbb{Z}$ denote the right hand side of the equation in the statement. Then for any $x \in \mathbb{Z}_2^{k-1}$

$$\begin{aligned} \hat{g}(x) &= \sum_{y \in \mathbb{Z}_2^{k-1}} f(y) \langle x, y \rangle \\ &= 2^{n-2}((a + b + \sum a_i) \langle x, 0 \rangle + \sum_i a_i \langle x, e_i \rangle + (a - b) \langle x, h \rangle). \end{aligned}$$

Now for all x , $\langle x, 0 \rangle = 1$, $1 + \langle x, e_i \rangle = 2x_i$ and $\langle x, h \rangle$ is 1 if $\sum_i x_i$ is even and -1 if $\sum_i x_i$ is odd. It follows that

$$\hat{g}(x) = \begin{cases} 2^{k-1}(a + \sum a_i x_i) & \text{if } \sum x_i \text{ is even} \\ 2^{k-1}(b + \sum a_i x_i) & \text{if } \sum x_i \text{ is odd} \end{cases}$$

$$= 2^{n-1}f(x)$$

Then g has the same fourier transform as \hat{f} and so must be equal to \hat{f} . \square

Then it follows that $f_{(a,b),(a_1,\dots,a_{k-1})}$ has a twin from which it has high distinguishing number.

Corollary 11. *For distinct non-negative integers a, b and positive integers a_1, \dots, a_{k-1} , the multisets $f_{(a,b),(a_1,\dots,a_{k-1})}$ and $f_{(b,a),(a_1,\dots,a_{k-1})}$ have distinguishing number k .*

Proof. By Theorem 10, the fourier transforms $g_1 = \hat{f}_{(a,b),a_1,\dots,a_{k-1}}$ and $g_2 = \hat{f}_{(b,a),b_1,\dots,b_{k-1}}$ have identical support $\{0, e_1, e_2, \dots, e_{k-1}, h\}$ and are equal except at $x = h$ for which we have $g_1(-x) = g_2(-x)$.

By Theorem 8, the distinguishing number of the two multisets is equal to the length of the minimum 0-sum sequence x_1, \dots, x_t for which

$$g_1(x_1) \dots g_1(x_t) \neq g_2(x_1) \dots g_2(x_t).$$

Clearly any such sequence must contain h an odd number of times, leaving a 1-coordinate in each location that must be made up by a copy of e_i . Thus the shortest such sequence has length k and is $e_1 + e_2 + \dots + e_{k-1} + h = 0$. \square

We will show that up to translation and linear maps on \mathbb{Z}_2^{k-1} , these are the only pairs of multisets of distinguishing number k . Say that two multisets f_1 and f_2 from \mathbb{Z}_2^{k-1} of distinguishing number k are in *standard position* if

$$\hat{f}_1 e_1 \dots \hat{f}_1 e_{k-1} \hat{f}_1 h \neq \hat{f}_2 e_1 \dots \hat{f}_2 e_{k-1} \hat{f}_2 h.$$

Theorem 12. *For $k \geq 3$, if f_1 and f_2 are two multisets on \mathbb{Z}_2^{k-1} of distinguishing number k , then there exists a bijective group homomorphism $\theta : \mathbb{Z}_2^{k-1} \rightarrow \mathbb{Z}_2^{k-1}$ such that θf_1 and θf_2 are in standard position.*

Proof. By Theorem 8, there is a 0-sum sequence of length k , x_1, \dots, x_k for which

$$\hat{f}_1(x_1) \dots \hat{f}_1(x_k) \neq \hat{f}_2(x_1) \dots \hat{f}_2(x_k),$$

and there is no shorter such sequence.

In particular this means that x_1, \dots, x_k cannot be split into two shorter 0-sum sequences (for they would both have equal sums), so x_1, \dots, x_{k-1} must be linearly independent and therefore must span \mathbb{Z}_2^{k-1} . As such there is a bijective group homomorphism $\theta : \mathbb{Z}_2^{k-1} \rightarrow \mathbb{Z}_2^{k-1}$ for which $\theta^* e_i = x_i$ for all $1 \leq i \leq k-1$.

Then by Lemma 6, if we denote θf_1 and θf_2 by g_1 and g_2 , we have

$$\hat{g}_1(e_1) \dots \hat{g}_1(e_{k-1}) \hat{g}_1(h) \neq \hat{g}_2(e_1) \dots \hat{g}_2(e_{k-1}) \hat{g}_2(h),$$

and there is no shorter such sequence. \square

Theorem 13. *For $k \geq 3$, if f_1 and f_2 are two multisets on \mathbb{Z}_2^{k-1} of distinguishing number k in standard position, then there exist distinct non-negative integers a, b , positive integers a_1, \dots, a_{k-1} and elements $x_1, x_2 \in \mathbb{Z}_2^{k-1}$ such that*

$$\begin{aligned} x_1 + f_1 &= f_{(a,b),(a_1,\dots,a_{k-1})} \\ x_2 + f_2 &= f_{(b,a),(a_1,\dots,b_{k-1})} \end{aligned}$$

Proof. We know that

$$\hat{f}_1(e_1) \dots \hat{f}_1(e_{k-1}) \hat{g}_1(h) \neq \hat{f}_2(e_1) \dots \hat{f}_2(e_{k-1}) \hat{g}_2(h),$$

and there is no shorter such sequence. In particular, note that for all $x \in \mathbb{Z}_2^{k-1}$, $x + x = 0$ is a shorter sequence, so $\hat{g}_1(x)^2 = \hat{g}_2(x)^2$.

Now let x be any element of \mathbb{Z}_2^{k-1} other than $\{0, e_1, e_2, \dots, e_{k-1}, h\}$, and let $I = \{i : 1 \leq i \leq k-1, x_i = 1\}$ be the set of 1 coordinates of x . Note that by the choice of x , $2 \leq p \leq k-2$. As such, it follows that $\{e_i : i \in I\} \cup \{x\}$ and $\{e_i : i \notin I\} \cup \{h, x\}$ are both 0-sum subsets of length at most $k-1$, and so it follows that

$$\begin{aligned} \prod_{i \in I} \hat{g}_1(e_i) \hat{g}_1(x) &= \prod_{i \in I} \hat{g}_2(e_i) \hat{g}_2(x) \text{ and} \\ \prod_{i \notin I} \hat{g}_1(e_i) \hat{g}_1(h) \hat{g}_1(x) &= \prod_{i \notin I} \hat{g}_2(e_i) \hat{g}_2(h) \hat{g}_2(x). \end{aligned}$$

Multiplying these together we get

$$\prod_i \hat{g}_1(e_i) \hat{g}_1(h) \hat{g}_1(x)^2 = \prod_i \hat{g}_1(e_i) \hat{g}_2(h) \hat{g}_2(x)^2.$$

Since we know that $\hat{g}_1(x)^2 = \hat{g}_2(x)^2$ and

$$\hat{g}_1(e_1) \dots \hat{g}_1(e_{k-1}) \hat{g}_1(h) \neq \hat{g}_2(e_1) \dots \hat{g}_2(e_{k-1}) \hat{g}_2(h),$$

it follows that $\hat{g}_1(x) = \hat{g}_2(x) = 0$.

To summarize, \hat{g}_1 and \hat{g}_2 have no support outside of $\{0, e_1, \dots, e_{k-1}, h\}$, we have $\hat{g}_1(x)^2 = \hat{g}_2(x)^2$ for all x and

$$\hat{g}_1(e_1) \dots \hat{g}_1(e_{k-1}) \hat{g}_1(h) \neq \hat{g}_2(e_1) \dots \hat{g}_2(e_{k-1}) \hat{g}_2(h).$$

Now let $x_1 = \sum_{\hat{g}_1 e_i < 0} e_i$ and $x_2 = \sum_{\hat{g}_2 e_i < 0} e_i$. Then for all i , $g_1 \hat{+} x_1 e_i$ and $g_1 \hat{+} x_2 e_i$ are positive numbers with the same square, and so are equal.

Thus $g_1 \hat{+} x_1$ and $g_2 \hat{+} x_2$ are of the form given in Theorem 10 except that we have not shown that a, b are necessarily non-negative, or that any of $a, b, a_1, \dots, a_{k-1}$ are necessarily integers.

To that end, note that $a = g_1 + x_1(0)$, $b = g_2 + x_2(0)$ (and so they are indeed non-negative integers), and $a_i = g_1 + x_1(e_i) - g_2 + x_2(0)$, so is integral. \square

It follows that if we have k -distinguishable multisets, some element must appear k times.

Theorem 14. *For integers $k \geq 2$, if multisets f and g on \mathbb{Z}_2^{k-1} have distinguishing number k , some element appears with multiplicity at least k in f or g .*

Proof. By Theorem 13, f and g are translates of a linear image of some pair $f_{(a,b),(a_1,\dots,a_{k-1})}$ and $f_{(b,a),(b_1,\dots,b_{k-1})}$. The multiplicity of h in these two multisets is $a + a_1 + \dots + a_{k-1}$ and $b + a_1 + \dots + a_{k-1}$. Since each a_i is a positive integer, and a and b are distinct non-negative integers, one of these numbers is at least k . \square

This now allows us to prove our upper bound.

Corollary 15. *For positive integers n and k , if the reconstruction number of \mathbb{Z}_2^n is at least k , then $2^{n+1-k} \geq k$.*

Proof. Suppose that the reconstruction number of \mathbb{Z}_2^n is $t \geq k$. Then there exists two sets $S_1, S_2 \subseteq \mathbb{Z}_2^n$ that are t -distinguishable, but not $t-1$ -distinguishable.

Then by Theorem 9, there exists a map $\theta : \mathbb{Z}_2^n \rightarrow \mathbb{Z}_2^{t-1}$ such that the multisets $\theta S_1, \theta S_2$ from \mathbb{Z}_2^{t-1} are t -distinguishable, but not $t-1$ -distinguishable.

Finally, by Theorem 14, there must be some element of \mathbb{Z}_2^{t-1} that appears in θS_1 or θS_2 at least t times. Since each element of \mathbb{Z}_2^{t-1} only has 2^{n+1-t} inverse images, it follows that $2^{n+1-t} \geq t$.

Since $t \geq k$, we must have $2^{n+1-k} \geq 2^{n+1-t} \geq t \geq k$. \square

Tying everything together, we now have proved the precise value of the reconstruction number of the hypercube.

Corollary 16. *The reconstruction number of \mathbb{Z}_2^n is*

$$\lfloor n + 1 - \log_2(n + 1 - \log_2(n)) \rfloor.$$

Proof. By Corollaries 5 and 15, the reconstruction number of \mathbb{Z}_2^n is the maximum value of k for which if $2^{n+1-k} \geq k$. By Theorem 1, this is $\lfloor n + 1 - \log_2(n + 1 - \log_2(n)) \rfloor$. \square

REFERENCES

- [1] NOGA ALON, YAIR CARO, ILIA KRASIKOV, and YEHUDA RODITTY. Combinatorial reconstruction problems. *Journal of Combinatorial Theory, Series B*, 47:153–161, 10 1989.
- [2] LUKE PEBODY. The reconstructibility of finite abelian groups. *Combinatorics, Probability and Computing*, 13:867–892, 11 2004.
- [3] JAMIE RADCLIFFE and ALEX SCOTT. Reconstructing subsets of \mathbb{Z}_n . *Journal of Combinatorial Theory, Series A*, 83:169–187, 8 1998.